

# Recipe 18 - Configuration Guide for Setting up Entrust GetAccess 7.0 SP 2 Patch 3 as an AA and CS

## Table of Contents:

1	Setup.....	1
1.1	Terms and Introduction .....	1
2	Partner Configuration.....	2
2.1	Open Entrust Directory for Configuration.....	2
2.2	Configure a Partner AA.....	3
2.2.1	Mapping Users.....	10
2.2.2	Mapping Usernames in Bulk .....	11
2.3	Configure a Partner CS.....	12

Version 3.0.0

## 1 Setup

### 1.1 Terms and Introduction

The SAML 1.0 is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML 1.0 and Entrust GetAccess v7.0 SP2 Patch 3 as an Agency Application (AA) and Credential Service (CS). Remember that the Entrust GetAccess setup screens are often the same, whether setting up an AA or a CS. After reviewing the terms, configure your scheme to handle SAML 1.0.

Term	Definition
Agency Application (AA)	An online service provided by a government agency that requires an end user to be authenticated.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential, then each one is considered a separate CS.
Credential Service Provider (CSP)	An organization that offers one or more CSs. Sometimes known as an Electronic Credential Provider (ECP).
Project Management Office (PMO)	The PMO is the organization that handles E-Authentication program management, administration, and operations.

## 2 Partner Configuration

### 2.1 Open Entrust Directory for Configuration

To open the Entrust directory for configuration, go to C:\Program Files\GetAccess\config\ and select configuration.global.xml as shown in figure 18-1.

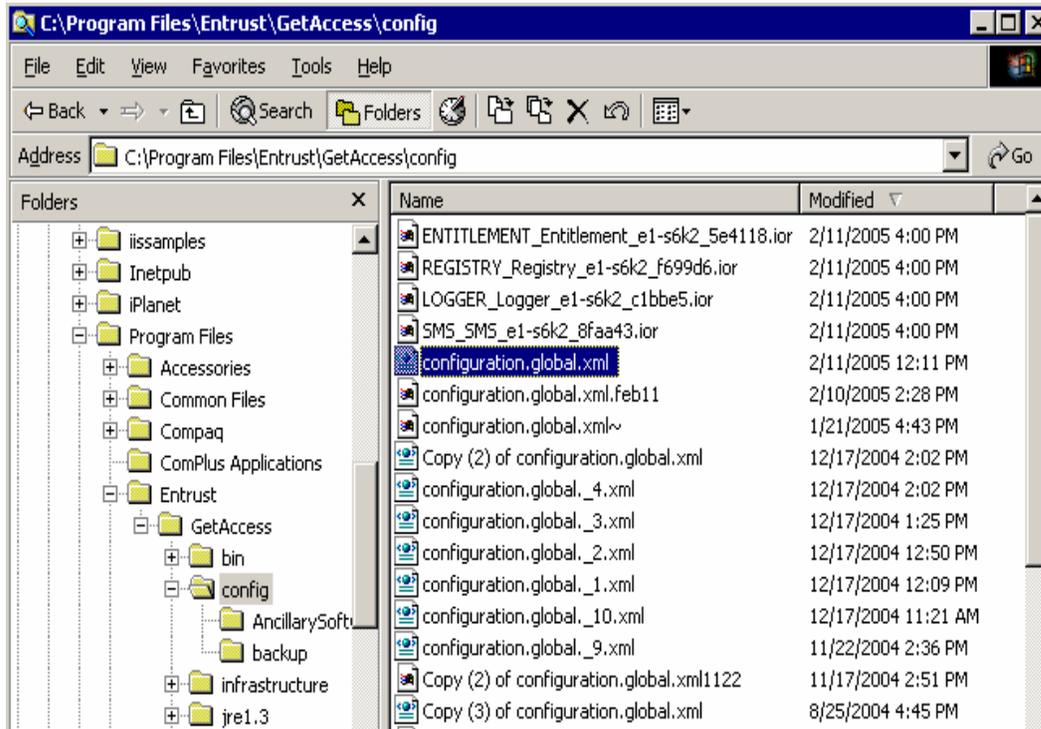


Figure 18-1: Entrust Directory

## 2.2 Configure a Partner AA

Once the configuration.global.xml file opens, find the <gaSamlPortalPartner></gaSamlPortalPartner> fields. An example of these fields are provided below.

```
<!-- site wide producing stuff -->
<gaSamlPortal>
<gaAssertionCache>gaStandardAssertionCache</gaAssertionCache>
<gaAssertionIssuer>http://e1-s6k2.caf.eauth.enspier.net</gaAssertionIssuer>
<gaAttributeNamespace>http://eauthentication.gsa.gov/federated/attribute</gaAttributeNamespace>
<gaAuthenticationAssertionGracePeriod>15</gaAuthenticationAssertionGracePeriod>
<gaAuthenticationAssertionLifetime>60</gaAuthenticationAssertionLifetime>
<gaSecurityDomain>http://e1-s6k2.caf.eauth.enspier.net</gaSecurityDomain>
<gaSubjectNameQualifier>e1-s6k2.caf.eauth.enspier.net</gaSubjectNameQualifier>

<!-- configuration to produce assertions for HP Phase1-->

<gaSamlPortalPartner>

    <gaPartnerAgentUrl>https://server1.interop1.eauth.enspier.net:9985/saml_in</gaPartnerAgentUrl
>

    <gaPartnerSecurityDomain>server1.interop1.eauth.enspier.net</gaPartnerSecurityDomain>
    <gaPortalSourceId>bc24b8e8d0d35c812092991c556faf5f64e15f05</gaPortalSourceId>
    <gaSignAuthenticationAssertion>false</gaSignAuthenticationAssertion>
    <gaSignResponse>false</gaSignResponse>
    <gaSignedRequestRequired>false</gaSignedRequestRequired>
    <gaSamlAttributes>

    <gaAttributeNamespace>http://eauthentication.gsa.gov/federated/attribute</gaAttributeNamespac
e>
        <gaAttributeStatementEnabled>true</gaAttributeStatementEnabled>
    </gaSamlAttributes>
    <gaSamlSubject>
        <gaSubjectNameFormat>X509SubjectName</gaSubjectNameFormat>
        <gaSubjectNamePrefix>uid=</gaSubjectNamePrefix>
        <gaSubjectNameQualifier>e1-
s6k2.caf.eauth.enspier.net</gaSubjectNameQualifier>
        <gaSubjectNameSuffix>,ou=caf,o=gsa,c=us</gaSubjectNameSuffix>
    </gaSamlSubject>
</gaSamlPortalPartner>
</gaSamlPortal>
```

Be sure to create a comment line noting the AA below </gaSamlPortalPartner>.

Once you have created the comment line, copy all <gaSamlPortalPartner> fields from the existing Agency Application entity (SAML Portal Partner) configuration and paste inside <gaSamlPortal></gaSamlPortal>. An example of this is provided below.

```
<gaSamlPortalPartner>
  <gaPartnerAgentUrl>https://server1.interop1.eauth.enspier.net:9985/saml_in</gaPartnerAgentUrl>

  <gaPartnerSecurityDomain>server1.interop1.eauth.enspier.net</gaPartnerSecurityDomain>
    <gaPortalSourceId>bc24b8e8d0d35c812092991c556faf5f64e15f05</gaPortalSourceId>
    <gaSignAuthenticationAssertion>>false</gaSignAuthenticationAssertion>
    <gaSignResponse>>false</gaSignResponse>
    <gaSignedRequestRequired>>false</gaSignedRequestRequired>
    <gaSamlAttributes>
      <gaAttributeNamespace>http://eauthentication.gsa.gov/federated/attribute</gaAttributeNamespace>
        <gaAttributeStatementEnabled>>true</gaAttributeStatementEnabled>
      </gaSamlAttributes>
    <gaSamlSubject>
      <gaSubjectNameFormat>X509SubjectName</gaSubjectNameFormat>
      <gaSubjectNamePrefix>uid=</gaSubjectNamePrefix>
      <gaSubjectNameQualifier>e1-
s6k2.caf.eauth.enspier.net</gaSubjectNameQualifier>
      <gaSubjectNameSuffix>,ou=caf,o=gsa,c=us</gaSubjectNameSuffix>
    </gaSamlSubject>
  </gaSamlPortalPartner>
```

Next, from the copied and pasted <gaSamlPortalPartner> fields, remove the contents of the <gaPartnerAgentURL></gaPartnerAgentURL>, <gaPartnerSecurityDomain></gaPartnerSecurityDomain>, and <gaSubjectNameQualifier></gaSubjectNameQualifier> fields. An example of this is provided below.

```
<gaSamlPortalPartner>
  <gaPartnerAgentUrl> </gaPartnerAgentUrl>
  <gaPartnerSecurityDomain> </gaPartnerSecurityDomain>
  <gaPortalSourceId>bc24b8e8d0d35c812092991c556faf5f64e15f05</gaPortalSourceId>
  <gaSignAuthenticationAssertion>>false</gaSignAuthenticationAssertion>
  <gaSignResponse>>false</gaSignResponse>
  <gaSignedRequestRequired>>false</gaSignedRequestRequired>
  <gaSamlAttributes>
    <gaAttributeNamespace> http://eauthentication.gsa.gov/federated/attribute
gaAttributeNamespace>
    <gaAttributeStatementEnabled>>true</gaAttributeStatementEnabled>
  </gaSamlAttributes>
  <gaSamlSubject>
    <gaSubjectNameFormat>X509SubjectName</gaSubjectNameFormat>
    <gaSubjectNamePrefix>uid=</gaSubjectNamePrefix>
    <gaSubjectNameQualifier> </gaSubjectNameQualifier>
    <gaSubjectNameSuffix>,ou=caf,o=gsa,c=us</gaSubjectNameSuffix>
  </gaSamlSubject>
</gaSamlPortalPartner>
```

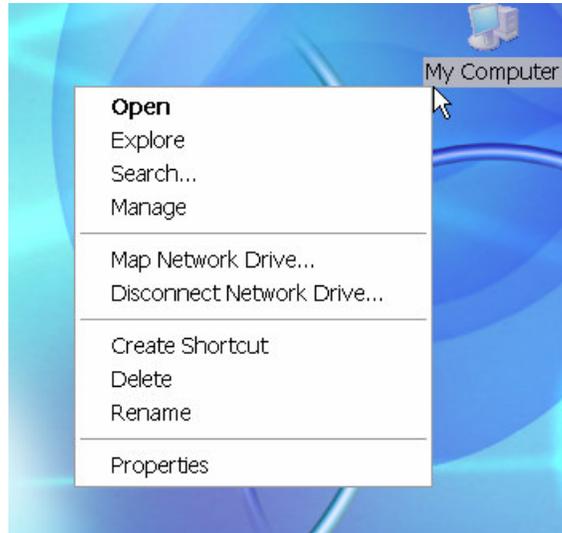
Once the contents have been erased, enter the correct configuration contents for <gaPartnerAgentURL> URL of the Agency Application entity ( SAML Portal Partner ) that will consume the SAML assertion </gaPartnerAgentURL>, <gaPartnerSecurityDomain> Name Qualifier (full computer name) of the AA entity (SAML Portal Partner) </gaPartnerSecurityDomain>, and <gaSubjectNameQualifier> Name Qualifier (full computer name) of the CS entity (SAML PartnerPortal) </gaSubjectNameQualifier>. An example of this is provided below.

```
<gaSamlPortalPartner>
    <gaPartnerAgentUrl>https://E1-
S2K3.caf.eauth.enspier.net:8443/artifact</gaPartnerAgentUrl>
    <gaPartnerSecurityDomain>e1-s2k3.caf.eauth.enspier.net</gaPartnerSecurityDomain>
    <gaPortalSourceId>bc24b8e8d0d35c812092991c556faf5f64e15f05</gaPortalSourceId>
    <gaSignAuthenticationAssertion>>false</gaSignAuthenticationAssertion>
    <gaSignResponse>>false</gaSignResponse>
    <gaSignedRequestRequired>>false</gaSignedRequestRequired>
    <gaSamlAttributes>
        <gaAttributeNamespace> http://eauthentication.gsa.gov/federated/attribute
    </gaAttributeNamespace>
        <gaAttributeStatementEnabled>>true</gaAttributeStatementEnabled>
    </gaSamlAttributes>
    <gaSamlSubject>
        <gaSubjectNameFormat>X509SubjectName</gaSubjectNameFormat>
        <gaSubjectNamePrefix>uid=</gaSubjectNamePrefix>
        <gaSubjectNameQualifier>e1-
s6k2.caf.eauth.enspier.net</gaSubjectNameQualifier>
        <gaSubjectNameSuffix>,ou=caf,o=gsa,c=us</gaSubjectNameSuffix>
    </gaSamlSubject>
</gaSamlPortalPartner>
```

Note the following:

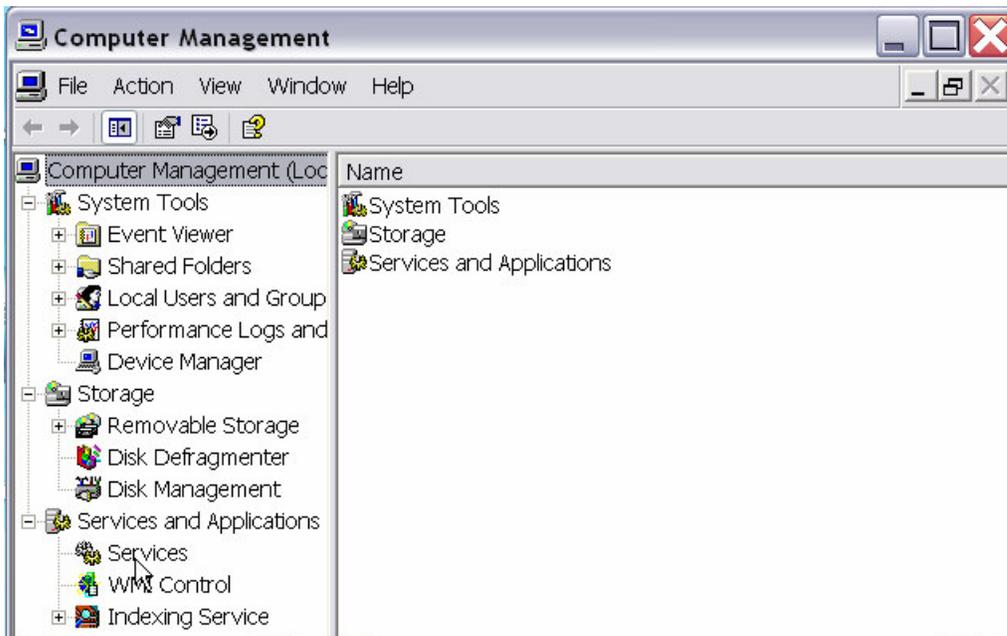
```
<gaPortalSourceId> - Does not need to be configured (use source ID of Entrust) </gaPortalSourceId>
<gaSignAuthenticationAssertion> - always "false" </gaSignAuthenticationAssertion>
<gaSignResponse> - always "false" </gaSignResponse>
<gaAttributeStatementEnabled> - always "true" </gaAttributeStatementEnabled>
<gaSubjectNameFormat> - always "X509SubjectName" </gaSubjectNameFormat>
<gaSubjectNamePrefix> - always "uid=" </gaSubjectNamePrefix>
<gaSubjectNameSuffix> - Does not need to be configured ("o=gsa, c=us" will work)
</gaSubjectNameSuffix>
```

Next, save and close the xml file, and then restart the Entrust service. From the desktop, right click on **My Computer** and select **Manage** as demonstrated in Figure 18-2.



**Figure 18-2: My Computer**

The Computer Management screen should appear as shown in Figure 18-3. From the left panel of the screen, expand **Services and Applications** and select **Services**.



**Figure 18-3: Computer Management**

The Services screen should appear as shown in Figure 18-4. In the right panel of the screen select **Entrust GetAccess**, right click on **Entrust GetAccess**, and select **Stop**. An example of this is provided below.

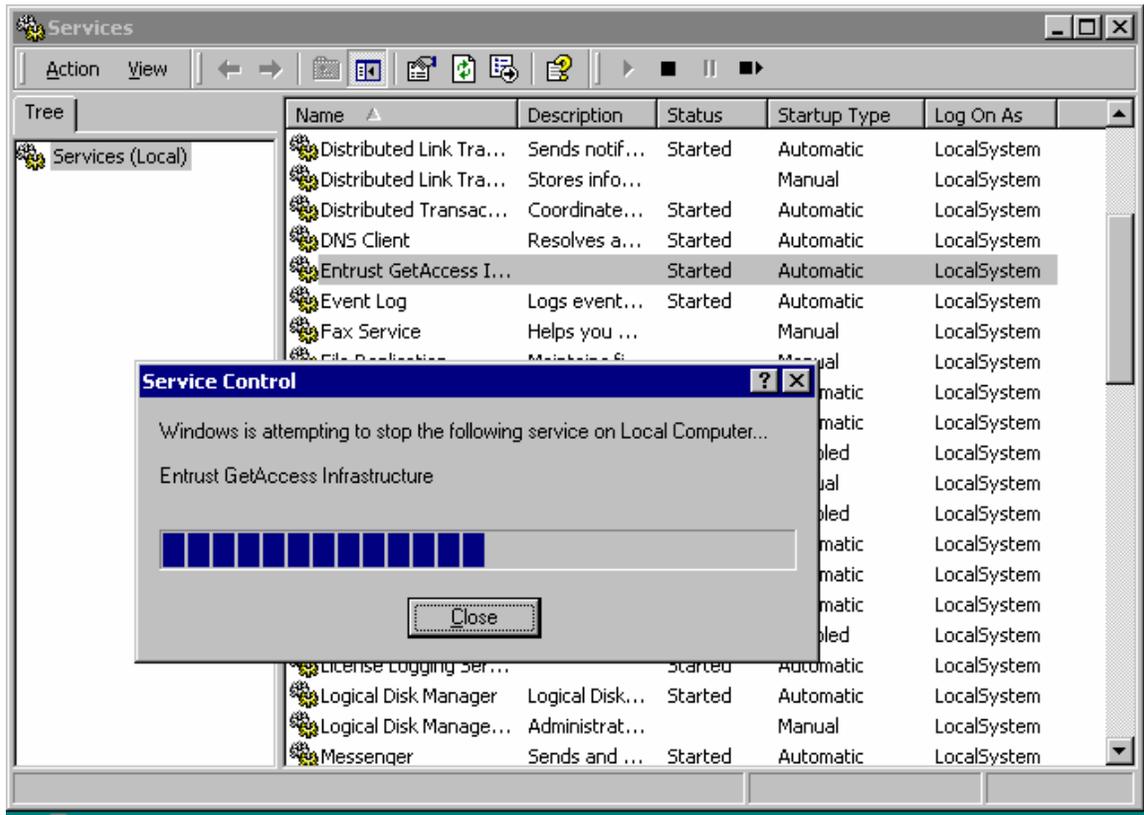


Figure 18-4: Services

Once the service has been stopped, right click on **Entrust GetAccess** again and select **Start**. “Started” should appear in the status column for Entrust GetAccess. Once that occurs, simply close the window.

### 2.2.1 Mapping Users

Next, users need to be mapped because domains are separate and do not share a common database of user information. Users require usernames on both the portal (CS) and partner (AA) domains to perform single sign-on. Typically a user may be identified with different usernames in different domains, so the partner must translate the portal username into a local partner username.

Complete the following steps in the Entrust GetAccess partner domain to map portal usernames to partner usernames one at a time.

Open Entrust GetAccess Server and in the partner domain open a command prompt and enter <GA\_root>\bin. In the command prompt, type:

```
runGaSAMLUseridMap -add -partnerUserId=<partnerUserId>  
-portalDomain=<portalDomain (CS)> -portalUserId=<portalUserId >
```

There are instances when a user is identified by “Bob” at the CS and identified as “Robert” at the AA. The partner servlet at the AA would need to translate “Bob” into “Robert” before logging the user in automatically.

In this case, type the command:

```
runGaSAMLUseridMap -add -partnerUserId=Robert -portalDomain="o=u.s. government, c=us" (the  
NameQualifier from the credential service metadata )-portalUserId="uid=bob, ou=gsa, o=u.  
s. government, c=us" ( This is NameIdentifier information, derived from the directory that the CS uses ).
```

An example of this is provided in Figure 18-5.

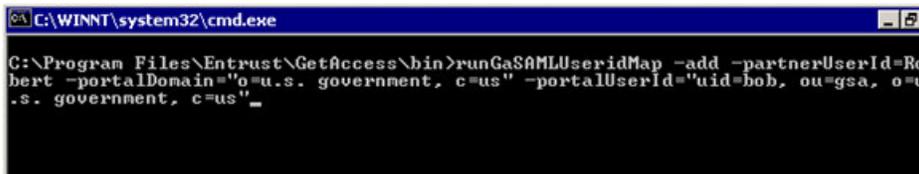


Figure 18-5: Mapping Users

Once the command has been entered, simply exit the command prompt.

### 2.2.2 Mapping Usernames in Bulk

To map usernames in bulk, open the partner site and create a XML file that contains a list of users using the following format:

```
<GaSamlUserMap>
<GaSamlPortal PortalDomain="partnerAdomain.com">
<GaSamlUser PortalUserId="portalusername"
PartnerUserId="partnerAusername"/>
...
</GaSamlPortal>
<GaSamlPortal PortalDomain="partnerBdomain.com">
<GaSamlUser PortalUserId="portalusername"
PartnerUserId="partnerusername"/>
...
</GaSamlPortal>
...
</GaSamlUserMap>
```

Note the following:

- The PortalDomain refers to the partner's security domain.
- PortalUserId refers to the Portal username. By default this would be Entrust GetAccess username; however, you can also configure the Subject Name format, in which the PortalUserId is the partner username for the user.

When complete, store this file in the <GA\_root>/bin folder. Next, open a command prompt, go to the <GA\_root>/bin directory, and run the GASAMLUseridMap script with the following parameters:

```
java GASAMLUseridMap -bulkadd -bulusersInputFile=file.xml
```

File.xml refers to the name of the XML file that contains the mapping information.

## 2.3 Configure a Partner CS

Open the configuration.global.xml file as previously described (Figure 18-1), and then find the <gaSamlPartnerPortal></gaSamlPartnerPortal> fields. An example of these fields are provided below.

```
<!-- site wide producing stuff -->
<gaSamlPartner>
    <gaByPassMappingAllowed>true</gaByPassMappingAllowed>
    <gaSecurityDomain>e1-s6k7.caf.eauth.enspier.net</gaSecurityDomain>

    <!-- configuration to consume assertions for HP Phase2-->
    <gaSamlPartnerPortal>
        <gaClientAuthenticationEnabled>true</gaClientAuthenticationEnabled>
        <gaClientCertAlias>e1s6k2_client</gaClientCertAlias>
        <gaPortalAgentUrl>https://e1-
s4k1.caf.eauth.enspier.net:9984/saml_responder/</gaPortalAgentUrl>
        <gaPortalCAAlias>egov.CS.CA</gaPortalCAAlias>
        <gaPortalSecurityDomain>E1-S4K1.caf.eauth.enspier.net</gaPortalSecurityDomain>
        <gaPortalSourceId>0b043b663783a9c5b71c3deb7e506c79fb4c95d7</gaPortalSourceId>
        <gaSamlVersion>1.0</gaSamlVersion>
        <gaServerAuthenticationEnabled>>false</gaServerAuthenticationEnabled>
        <gaSignRequest>>false</gaSignRequest>

        <gaSignedAuthenticationAssertionRequired>>false</gaSignedAuthenticationAssertionRequired>
        <gaSignedResponseRequired>>false</gaSignedResponseRequired>
        <gaSslDebugEnabled>>false</gaSslDebugEnabled>
    </gaSamlPartnerPortal>
</gaSamlPartner>
```

Be sure to create a comment line noting the CS below </gaSamlPartnerPortal>.

Once you have created the comment line, copy all <gaSamlPartnerPortal> fields from the existing CS entity (SAML Partner Portal) configuration and paste inside <gaSamlPartner></gaSamlPartner>. An example of this is provided below.

```
<!--configuration to consume assertions for Entegrity Phase2-->
  <gaSamlPartnerPortal>
    <gaClientAuthenticationEnabled>true</gaClientAuthenticationEnabled>
    <gaClientCertAlias>e1s6k2_client</gaClientCertAlias>
    <gaPortalAgentUrl>https://E1-
S2K3.caf.eauth.enspier.net:8083/responder</gaPortalAgentUrl>
    <gaPortalCAAlias>egov.CS.CA</gaPortalCAAlias>
    <gaPortalSecurityDomain>http://E1-
S2K3.caf.eauth.enspier.net</gaPortalSecurityDomain>
    <gaPortalSourceId>4d2ed66731aa42f26781db4340efb3b0925f5a94</gaPortalSourceId>
    <gaSamlVersion>1.0</gaSamlVersion>
    <gaServerAuthenticationEnabled>>false</gaServerAuthenticationEnabled>
    <gaSignRequest>>false</gaSignRequest>

    <gaSignedAuthenticationAssertionRequired>>false</gaSignedAuthenticationAssertionRequired>
    <gaSignedResponseRequired>>false</gaSignedResponseRequired>
    <gaSslDebugEnabled>>false</gaSslDebugEnabled>
  </gaSamlPartnerPortal>
```

Next, from the copied and pasted <gaSamlPartnerPortal> fields, remove the contents of the <gaPortalAgentUrl></gaPortalAgentUrl>, <gaPortalSecurityDomain></gaPortalSecurityDomain>, and <gaPortalSourceId></gaPortalSourceId> fields. An example of this is provided below.

```
<!--configuration to consume assertions for Entegrity Phase2-->
  <gaSamlPartnerPortal>
    <gaClientAuthenticationEnabled>true</gaClientAuthenticationEnabled>
    <gaClientCertAlias>e1s6k2_client</gaClientCertAlias>
    <gaPortalAgentUrl> </gaPortalAgentUrl>
    <gaPortalCAAlias>egov.CS.CA</gaPortalCAAlias>
    <gaPortalSecurityDomain> <gaPortalSecurityDomain>
    <gaPortalSourceId></gaPortalSourceId>
    <gaSamlVersion>1.0</gaSamlVersion>
    <gaServerAuthenticationEnabled>>false</gaServerAuthenticationEnabled>
    <gaSignRequest>>false</gaSignRequest>

    <gaSignedAuthenticationAssertionRequired>>false</gaSignedAuthenticationAssertionRequired>
    <gaSignedResponseRequired>>false</gaSignedResponseRequired>
    <gaSslDebugEnabled>>false</gaSslDebugEnabled>
  </gaSamlPartnerPortal>
```

Once the contents have been erased, enter the correct configuration contents for <gaPartnerAgentUrl> URL of the CS entity (SAML Partner Portal) that will produce the SAML assertion </gaPartnerAgentUrl>, <gaPortalSecurityDomain> Name Qualifier (full computer name) of the CS entity (SAML Partner Portal) </gaPortalSecurityDomain>, and <gaPortalSourceID> SHA-1 or Base 64 encoding of the Name Qualifier (issuer name) </gaPortalSourceID>. An example of this is provided below.

```

<!--configuration to consume assertions for Entegrity -->
  <gaSamlPartnerPortal>
    <gaClientAuthenticationEnabled>true</gaClientAuthenticationEnabled>
    <gaClientCertAlias>e1s6k2_client</gaClientCertAlias>
    <gaPortalAgentUrl>https://E1-
S2K3.caf.eauth.enspier.net:8083/responder</gaPortalAgentUrl>
    <gaPortalCAAlias>egov.CS.CA</gaPortalCAAlias>
    <gaPortalSecurityDomain>http://E1-
S2K3.caf.eauth.enspier.net</gaPortalSecurityDomain>

    <gaPortalSourceId>4d2ed66731aa42f26781db4340efb3b0925f5a94</gaPortalSourceId>
    <gaSamlVersion>1.0</gaSamlVersion>
    <gaServerAuthenticationEnabled>>false</gaServerAuthenticationEnabled>
    <gaSignRequest>>false</gaSignRequest>

    <gaSignedAuthenticationAssertionRequired>>false</gaSignedAuthenticationAssertionRequired>
    <gaSignedResponseRequired>>false</gaSignedResponseRequired>
    <gaSslDebugEnabled>>false</gaSslDebugEnabled>
  </gaSamlPartnerPortal>

```

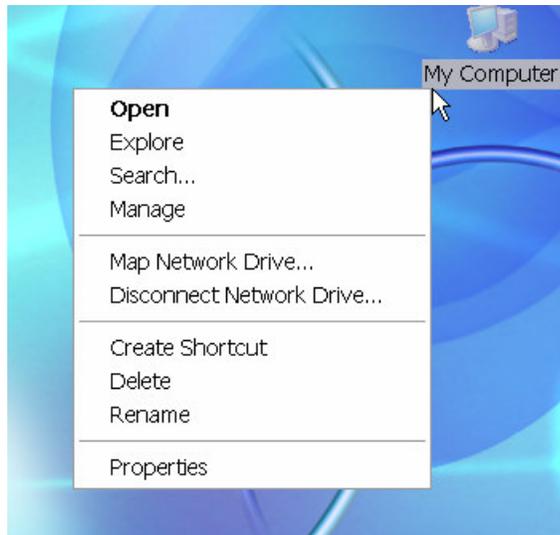
Note the following:

```

<gaClientAuthenticationEnabled>- always "true"</gaClientAuthenticationEnabled>
<gaClientCertAlias>e1s6k2_client (Agency Application entity)</gaClientCertAlias>
<gaPortalCAAlias>egov.CS.CA (Credential Service Provider CA)</gaPortalCAAlias>
<gaSamlVersion>1.0 (SAML version)</gaSamlVersion>
<gaServerAuthenticationEnabled>-always "false"</gaServerAuthenticationEnabled>
<gaSignRequest>- always "false"</gaSignRequest>
<gaSignedAuthenticationAssertionRequired>-always "false"</gaSignedAuthenticationAssertionRequired>
<gaSignedResponseRequired>-always "false"</gaSignedResponseRequired>
<gaSslDebugEnabled>-always "false"</gaSslDebugEnabled>
</gaSamlPartnerPortal>

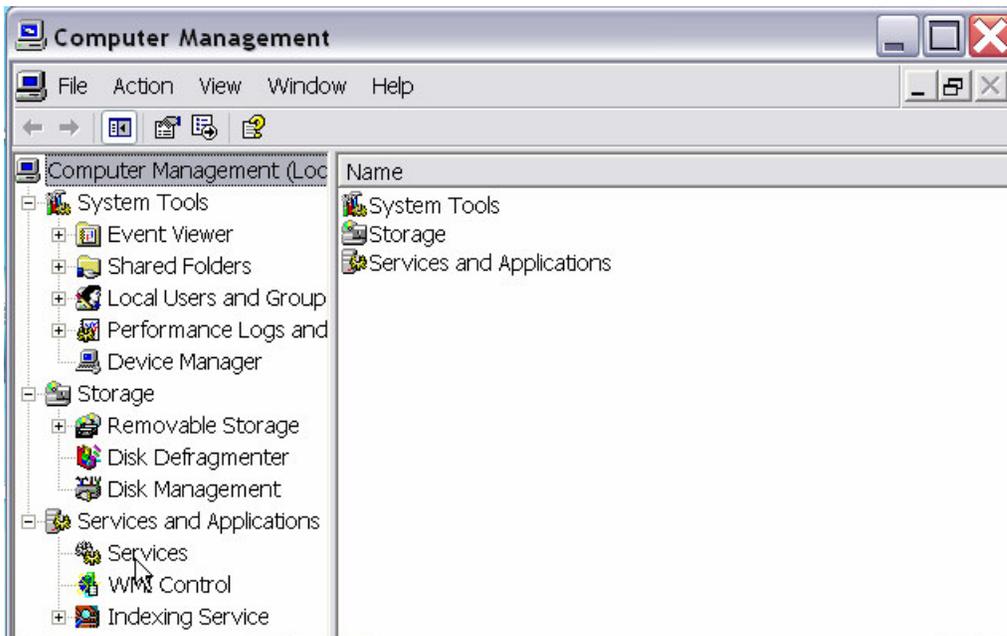
```

Next, save and close the xml file, and then restart the Entrust service. As demonstrated in Figure 18-6, right click on **My Computer** and select **Manage**.



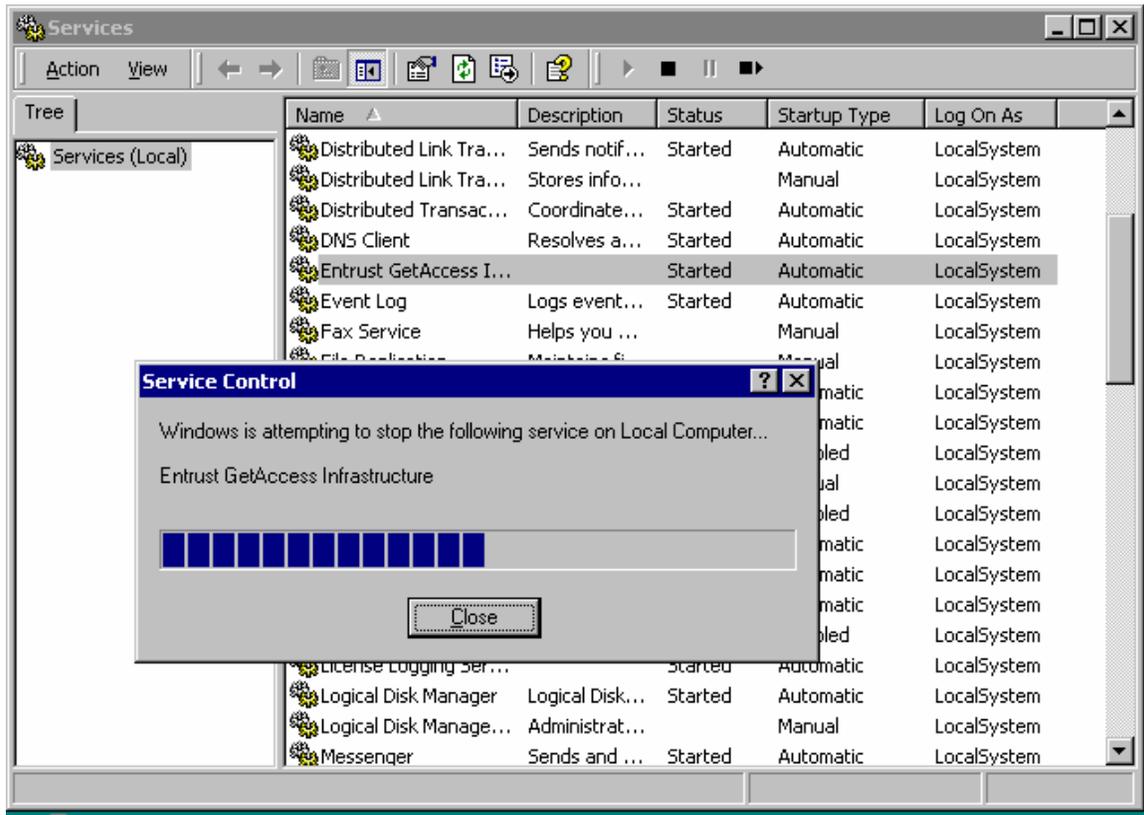
**Figure 18-6: My Computer**

The Computer Management screen will appear as shown in Figure 18-7. Next, from the left panel of the screen, expand **Services and Applications**, and then select **Services**.



**Figure 18-7: Computer Management**

The Services screen will appear as shown in Figure 18-8. In the right panel of the screen, right click on **Entrust GetAccess** and select **Stop**. An example of this is provided below.



**Figure 18-8: Services**

Once the service has been stopped, right click on Entrust GetAccess again and select Start. “Started” should appear in the status column for Entrust GetAccess. Close the window.